PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : H04B 7/00

A2

(11) Internationale Veröffentlichungsnummer: WO 00/14895

(43) Internationales Veröffentlichungsdatum: 16. März 2000 (16.03.00)

(21) Internationales Aktenzeichen: PCT/DE99/02836

(22) Internationales Anmeldedatum: 7. September 1999 (07.09.99)

(30) Prioritätsdaten:
198 40 742.4 7. September 1998 (07.09.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: DE-TEMOBIL DEUTSCHE TELEKOM MOBILNET GMBH [DE/DE]; Landgrabenweg 151, D–53227 Bonn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: HAKE, Jens [DE/DE]; Südweg 4b, D–09240 Kemtau (DE). THELEN, Jörg [DE/DE]; Nesselroderstrasse 27, D–53227 Bonn (DE).

(81) Bestimmungsstaaten: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CZ, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht
Ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts.

(54) Title: METHOD FOR IMPROVING THE SECURITY OF AUTHENTICATION PROCEDURES IN DIGITAL MOBILE RADIO TELEPHONE SYSTEMS

(54) Bezeichnung: VERFAHREN ZUR ERHÖHUNG DER SICHERHEIT VON AUTHENTISIERUNGSVERFAHREN IN DIGITALEN MOBILFUNKSYSTEMEN

(57) Abstract

The invention relates to a method for improving the security of authentication procedures in digital mobile radio telephone systems. In order to make it more difficult if not impossible to work out a secret code KI, several different secret SIM–specific codes KI are contained in the mobile radio telephone network and on a subscriber identity module SIM and a code KI for the implementation of said authentication is selected from the various secret codes thus contained during the authentication process between the subscriber identity module and the mobile radio telephone system pertaining to said SIM.

(57) Zusammenfassung

Die Erfindung betrifft ein Verfahren zur Erhöhung der Sicherheit von Authentisierungsverfahren in digitalen Mobilfunksystemen. Um ein Ausspähen des geheimen Schlüssels KI zu erschweren, bzw. nahezu unmöglich zu machen, wird vorgeschlagen, dass im Mobilfunknetz und auf einem Teilnehmeridentitätsmodul mehrere verschieden geheime, SIM–spezifische Schlüssel KI vorgehalten werden, und bei der Authentisierung zwischen dem Teilnehmeridentitätsmodul und dem Mobilfunknetz von oder SIM aus den mehreren vorgehaltenen geheimen Schlüsseln ein Schlüssel KI für die Durchführung der Authentisierung ausgewählt wird.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische Republik Mazedonien	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland			**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von Amerika
CA	Kanada	**IT**	Italien	**MX**	Mexiko		
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik Korea	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun			**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Beschreibung

Verfahren zur Erhöhung der Sicherheit von Authentisierungsverfahren in digitalen Mobilfunksystemen

Die Erfindung betrifft ein Verfahren zur Erhöhung der Sicherheit von Authentisierungsverfahren in digitalen Mobilfunksystemen nach dem Oberbegriff des Patentanspruchs 1.

Moderne Mobilfunknetze beinhalten spezielle Sicherheitsmassnahmen, die einen Missbrauchsschutz von Betriebsmitteln durch andere, als die autorisierten Teilnehmer, sowie Schutz vor einem möglichen Abhören der Funkschnittstelle beinhalten. Die Sicherheitsmassnahmen beziehen sich dabei auf den Schutz der Beziehung zwischen Mobilfunknetz und autorisiertem Teilnehmer. Ein spezielles Verfahren zur Authentisierung der Teilnehmer soll verhindern, dass ein Dritter die Identität eines autorisierten Teilnehmers vortäuschen kann. Ein Teilnehmer muss sich dazu mittels der auf seinem Teilnehmeridentitätsmodul (SIM) gespeicherten Daten und Funktionen gegenüber dem Mobilfunknetz authentifizieren. Es hat sich in der Vergangenheit immer wieder gezeigt, dass das Kompromitieren von Authentisierungsverfahren, d.h. das Ausspähen des geheimen Schlüssels KI des Teilnehmers mit entsprechendem Fachwissen und geeigneten Gerätschaften möglich ist, indem Folgen von den bei der Authentisierung verwendeten Zufallszahlen und Antwortzahlen, d.h. RAND/SRES-Paaren, in grosser Anzahl mathematischen Verfahren unterzogen werden, um

den geheimen Schlüssel KI eines Teilnehmers zu ermitteln. Ist der geheime Schlüssel KI erst einmal ermittelt, ist eine illegale Duplizierung von Teilnehmeridentitätsmodulen (SIMs) möglich.

Bei dem derzeit angewendeten Authentisierungsverfahren ermittelt das Mobilfunknetz mit speziellen Algorithmen und einem SIM-spezifischen, geheimen Schlüssel KI aus einem Zufallswert RAND ein Authentisierungsergebnis SRES und einen temporären Schlüssel KC. Dabei hält das Mobilfunknetz eine bestimmte Anzahl von RAND/SRES/KC-Triplets vor. will sich ein Teilnehmer einbuchen, sendet das Mobilfunknetz eine Zufallszahl RAND an das Teilnehmeridentitätsmodul SIM. Die SIM ermittelt mit dem gleichen, speziellen Algorithmus und seinem SIM-spezifischen, geheimen Schlüssel KI ein dazugehörendes SRES/KC-Paar und sendet die ermittelte SRES zurück an das Mobilfunknetz. Das Mobilfunknetz vergleicht die empfangene SRES mit der vorgehaltenen SRES auf Übereinstimmung, wobei bei Übereinstimmung der Teilnehmer als authentifiziert gilt. Der auf beiden Seiten berechnete Schlüssel KC wird auf beiden Seiten zur Verschlüsselung der Übertragung verwendet.

Wie gesagt besteht bei dem derzeit verwendeten Verfahren die Möglichkeit, den Schlüssel KI auszuspähen, um so unbefugt Zugang zum Mobilfunknetz zu erhalten.

Der vorliegenden Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren zur Erhöhung der Sicherheit von Authentisierungsverfahren in digitalen Mobilfunksystemen vorzuschlagen, durch welches das Ausspähen des geheimen Schlüssels nahezu unmöglich wird.

Diese Aufgabe wird durch die kennzeichnenden Merkmale des Patentanspruchs 1 gelöst.

Die Erfindung beruht nun darauf, dass im Mobilfunknetz und auf dem Teilnehmeridentitätsmodul mehrere verschiede geheime, SIM-spezifische Schlüssel KI vorgehalten werden, und bei der Authentisierung zwischen Teilnehmeridentitätsmodul und Mobilfunknetz aus den mehreren vorgehaltenen geheimen Schlüsseln ein Schlüssel für die Durchführung der Authentisierung ausgewählt wird.

Der Vorteil dieses Verfahrens liegt darin, dass ein Kompromitieren, d.h. ein Ausspähen des geheimen Schlüssels KI der SIM wesentlich erschwert wird, da für den Angreifer nicht vorhersehbar und nicht erkennbar ist, welcher geheime Schlüssel KI von der SIM zur Errechnung der SRES-Antwort verwendet wurde.

Weiterer wesentlicher Vorteil dieses Verfahrens ist, dass eine Änderung an den Schnittstellen des Mobilfunknetzes, insbesondere der Luftschnittstelle, nicht erforderlich ist, und ebenso keine Änderungen an den Endgeräten vorgenommen werden müssen. Es sind lediglich lokale softwaretechnische Änderungen an einzelnen Netzkomponenten des Mobilfunknetzes sowie auf der SIM erforderlich, die mit geringem Aufwand und nahezu ohne zusätzliche Kosten durchführbar sind.

Vorteilhafte Weiterbildungen und Ausführungsformen der Erfindung sind in den abhängigen Patentansprüchen angegeben.

Vorteilhaft erfolgt die Auswahl des verwendeten Schlüssels KI durch die SIM nach dem Zufallsprinzip.

In einer bevorzugten Ausführung ermittelt das Mobilfunknetz mit speziellen Algorithmen unter Vorgabe jeweils einer Zufallszahl RAND für alle SIM-spezifischen Schlüssel KI eines Teilnehmers ein SRES/KC-Paar und bildet mit dem jeweils verwendeten RAND die sogenannten RAND/SRES/KC-Triplets. Diese Triplets werden im Mobilfunknetz vorgehalten und sind für zukünftige Authentisierungsprozeduren abrufbar.

Zur Initiierung einer Authentisierung sendet das Mobilfunknetz einen Zufallswert RAND eines dieser Triplets an das Teilnehmer-Identitätsmodul SIM, wobei das Teilnehmeridentitätsmodul anhand der übermittelten RAND einen verfügbaren Schlüssel auswählt und anhand dieses ausgewählten Schlüssels KI die zugehörigen Werte für die Antwort SRES und den Schlüssel KC berechnet und die Antwort SRES an das Mobilfunknetz zurücksendet.

Im Mobilfunknetz findet nun ein Vergleich auf Übereinstimmung der empfangenen Antwort SRES mit allen für den verwendeten RAND vorgehaltenen SRES-Werten statt, wobei wenn eine Übereinstimmung zwischen zwei teilnehmerspezifischen Antworten SRES vorliegt der Teilnehmer als authentisiert gilt.

Vorteilhaft wird das Mobilfunknetz nun den zu den übereinstimmenden SRES gehörenden KC zur Verschlüsselung der Übertragung verwenden, wobei der identische Schlüssel KC in der SIM vorliegt und auch dort zur Verschlüsselung der Übertragung verwendet wird.

Nachfolgend wird ein Ausführungsbeispiel der Erfindung anhand einer Zeichnungsfigur näher erläutert. Dabei gehen aus der

Zeichnung und der zugehörigen Beschreibung weitere Merkmale und Vorteile der Erfindung hervor.

Figur 1 zeigt in vereinfachter Darstellung eine Authentisierungsprozedur nach dem erfindungsgemässen Verfahren. Zur Durchführung des Verfahrens müssen für jeden Teilnehmer im Mobilfunknetz als auch auf der teilnehmerspezifischen SIM mehrere geheime Schlüssel KI abgelegt sein.

Mobilfunknetz: Teilnehmer X

	KI 1	KI 2	KI 3
RAND 1	SRES/KC (1,1)	SRES/KC (1,2)	SRES/KC (1,3)
RAND 2	SRES/KC (2,1)	SRES/KC (2,2,)	SRES/KC (2,3)
RAND 3	SRES/KC (3,1)	SRES/KC (3,2)	SRES/KC (3,3)
...	...	...	...

Wie die obenstehende Tabelle zeigt sind im Mobilfunknetz für jeden Teilnehmer X beispielsweise drei geheime Schlüssel KI abgelegt, wobei nun das Mobilfunknetz unter Vorgabe von mehreren Zufallszahlen RAND 1, RAND 2 und RAND 3 die für jeweils die geheimen Schlüssel KI 1, KI 2 und KI 3 zugehörigen SRES-Antworten und Schlüssel KC berechnet und abspeichert.

Auch im Teilnehmeridentitätsmodul für den Teilnehmer X sind die drei möglichen Schlüssel KI 1, KI 2 und KI 3 abgelegt.

Will sich der Teilnehmer X nun im Mobilfunknetz einbuchen, so muss zunächst die Authentisierungsprozedur durchgeführt

werden, wie sie in Figur 1 angedeutet ist. Dazu sendet das Teilnehmeridentitätsmodul über ein entsprechendes Endgerät zunächst die Teilnehmeridentitätsnummer IMSI an das Mobilfunknetz. Wird diese IMSI als zulässig erkannt, dann wählt das Mobilfunknetz aus den für den Teilnehmer X vorgehaltenen Zufallswerten RAND einen Zufallswert, hier beispielsweise RAND 3, aus und sendet diesen zurück an das Teilnehmeridentitätsmodul. Das Teilnehmeridentitätsmodul wählt wiederum einen der teilnehmerspezifischen, geheimen Schlüssel KI aus, beispielsweise KI 2, und berechnet aus der vom Mobilfunknetz erhaltenen RAND 3 und dem KI 2 die zugehörige SRES-Antwort und den Schlüssel KC. Die SRES-Antwort, die aus dem Schlüssel KI 2 und der RAND 3 gebildet wurde, wird wieder zurück an das Mobilfunknetz gesendet und dort mit dem vorgehaltenen SRES-Wert für KI 2 und RAND 3 verglichen. Stimmen diese SRES-Werte überein, so gilt der Teilnehmer als authentisiert und kann sich in das Mobilfunknetz einbuchen. Der auf beiden Seiten vorliegende Schlüssel KC wird während der neu hergestellten Verbindung zur Verschlüsselung der Datenübertragung verwendet.

Patentansprüche

1. Verfahren zur Erhöhung der Sicherheit von Authentisierungsverfahren in digitalen Mobilfunksystemen, **dadurch gekennzeichnet**,
daß im Mobilfunknetz und auf einem Teilnehmeridentitätsmodul (SIM) mehrere verschiedene geheime, SIM-spezifische Schlüssel (KI) vorgehalten werden, und bei der Authentisierung zwischen Teilnehmeridentitätsmodul und Mobilfunknetz von der SIM aus den mehreren, vorgehaltenen geheimen Schlüsseln ein Schlüssel (KI) für die Durchführung der Authentisierung ausgewählt wird.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, daß die Auswahl des Schlüssels (KI) durch das Teilnehmeridentitätsmodul SIM nach dem Zufallsprinzip erfolgt.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, daß das Mobilfunknetz mit speziellen Algorithmen unter Vorgabe einer Zufallszahl (RAND) für alle SIM-spezifischen Schlüssel (KI) ein SRES/KC-Paar ermittelt, die mit dem jeweiligen RAND RAND/SRES/KC-Triplets bilden.

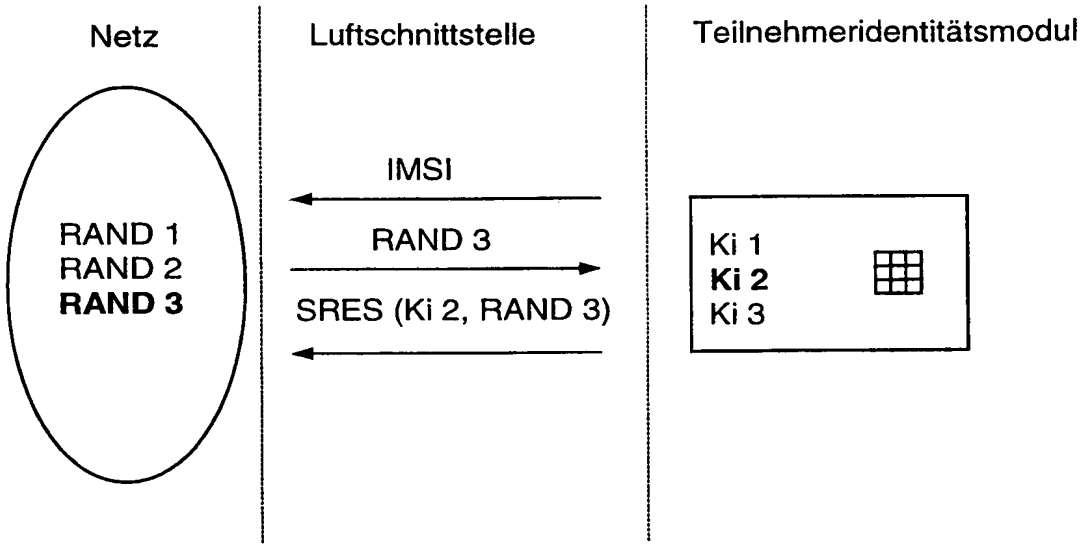
4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet**, daß die gebildeten RAND/SRES/KC-Triplets im Mobilfunknetz vorgehalten werden.

5. Verfahren nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet**, daß vom Mobilfunknetz zur Initiierung einer Authentisierung ein RAND eines dieser Triplets an das Teilnehmeridentitätsmodul gesendet wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet**, daß das Teilnehmeridentitätsmodul anhand der übermittelten RAND und dem ausgewählten Schlüssel (KI) die zugehörigen Werte für SRES und KC berechnet, und die ermittelte Antwort an das Mobilfunknetz sendet.

7. Verfahren nach einem der Ansprüche 1 bis 6, **dadurch gekennzeichnet**, daß im Mobilfunknetz ein Vergleich auf Übereinstimmung der empfangenen SRES mit allen für den verwendeten RAND vorgehaltenen SRES stattfindet.

8. Verfahren nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet**, daß das Mobilfunknetz und die SIM den zu dem übereinstimmenden SRES gehörenden KC zur Verschlüsselung der Übertragung verwendet.


Netz
Luftschnittstelle
Teilnehmeridentitätsmodul
RAND 1
RAND 2
RAND 3
IMSI
RAND 3
SRES (Ki 2, RAND 3)
Ki 1
Ki 2
Ki 3

FIGUR 1